

**This Page is Inserted by IFW Indexing and Scanning
Operations and is not part of the Official Record**

BEST AVAILABLE IMAGES

Defective images within this document are accurate representations of the original documents submitted by the applicant.

Defects in the images include but are not limited to the items checked:

- ☐ **BLACK BORDERS**
- ☐ **IMAGE CUT OFF AT TOP, BOTTOM OR SIDES**
- ☐ **FADED TEXT OR DRAWING**
- ☐ **BLURRED OR ILLEGIBLE TEXT OR DRAWING**
- ☐ **SKEWED/SLANTED IMAGES**
- ☐ **COLOR OR BLACK AND WHITE PHOTOGRAPHS**
- ☐ **GRAY SCALE DOCUMENTS**
- ☐ **LINES OR MARKS ON ORIGINAL DOCUMENT**
- ☐ **REFERENCE(S) OR EXHIBIT(S) SUBMITTED ARE POOR QUALITY**
- ☐ **OTHER:** _____

IMAGES ARE BEST AVAILABLE COPY.

As rescanning these documents will not correct the image problems checked, please do not report these problems to the IFW Image Problem Mailbox.

[Subscribe \(Full Service\)](#) [Register \(Limited Service, Free\)](#) [Login](#)Search: ☒ The ACM Digital Library ☐ The Guide

THE ACM DIGITAL LIBRARY

[Feedback](#) [Report a problem](#) [Satisfaction survey](#)Terms used **rsa hensel**

Found 2 of 142,983

Sort results
byDisplay
results[Save results to a Binder](#)[Search Tips](#)☐ Open results in a new
windowTry an [Advanced Search](#)Try this search in [The ACM Guide](#)

Results 1 - 2 of 2

Relevance scale ☐ ☐ ☐ ☐ ☐**1 Regular contributions: Architectural tradeoff in implementing RSA processors**

Fu-Chi Chang, Chia-Jiu Wang

March 2002 **ACM SIGARCH Computer Architecture News**, Volume 30 Issue 1Full text available: pdf(385.39 KB) Additional Information: [full citation](#), [abstract](#), [references](#), [index terms](#)

An investigation of a suite of RSA processors using different exponentiation and modular arithmetic algorithms is the main theme of this paper. The execution time and the amount of hardware required of different algorithms used to implement the RSA processor are compared. The modular algorithms examined in this paper are classical modular algorithm, Barrett's modular algorithm, Hensel's odd division and Montgomery's modular algorithm. The exponentiation algorithms implemented are the left-to-right ...

2 Book reviews: Modern computer algebra

R. Gregory Taylor

September 2002 **ACM SIGACT News**, Volume 33 Issue 3Full text available: pdf(893.78 KB) Additional Information: [full citation](#)

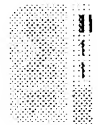
Results 1 - 2 of 2

The ACM Portal is published by the Association for Computing Machinery. Copyright © 2004 ACM, Inc.

[Terms of Usage](#) [Privacy Policy](#) [Code of Ethics](#) [Contact Us](#)Useful downloads: [Adobe Acrobat](#) [QuickTime](#) [Windows Media Player](#) [Real Player](#)

IEEE HOME | SEARCH IEEE | SHOP | WEB ACCOUNT | CONTACT IEEE


[Membership](#) | [Publications/Services](#) | [Standards](#) | [Conferences](#) | [Careers/Jobs](#)
IEEE Xplore
RELEASE 1.2

 Welcome
 United States Patent and Trademark Office


» See

[Help](#) | [FAQ](#) | [Terms](#) | [IEEE Peer Review](#)
[Quick Links](#)
Welcome to IEEE Xplore

- ☐ Home
- ☐ What Can I Access?
- ☐ Log-out

Tables of Contents

- ☐ Journals & Magazines
- ☐ Conference Proceedings
- ☐ Standards

Search

- ☐ By Author
- ☐ Basic
- ☐ Advanced

Member Services

- ☐ Join IEEE
- ☐ Establish IEEE Web Account
- ☐ Access the IEEE Member Digital Library

IEEE Enterprise

- ☐ Access the IEEE Enterprise File Cabinet

Print Format

[Home](#) | [Log-out](#) | [Journals](#) | [Conference Proceedings](#) | [Standards](#) | [Search by Author](#) | [Basic Search](#) | [Advanced Search](#) | [Join IEEE](#) | [Web Account](#) | [New this week](#) | [OPAC Linking Information](#) | [Your Feedback](#) | [Technical Support](#) | [Email Alerting](#) | [No Robots Please](#) | [Release Notes](#) | [IEEE Online Publications](#) | [Help](#) | [FAQ](#) | [Terms](#) | [Back to Top](#)

Copyright © 2004 IEEE — All rights reserved

Your search matched **2** of **1075719** documents.A maximum of **500** results are displayed, **15** to a page, sorted by **Relevance Descending** order.**Refine This Search:**

You may refine your search by editing the current search expression or enter a new one in the text box.

rsa <and> hensel

☐ Check to search within this result set**Results Key:****JNL** = Journal or Magazine **CNF** = Conference **STD** = Standard**1 Fast implementations of RSA cryptography**

Shand, M.; Vuillemin, J.;

Computer Arithmetic, 1993. Proceedings., 11th Symposium on , 29 June-2 July 1993

Pages:252 - 259

[\[Abstract\]](#) [\[PDF Full-Text \(516 KB\)\]](#) **IEEE CNF**
2 A systolic, linear-array multiplier for a class of right-shift algorithm

Kornerup, P.;

Computers, IEEE Transactions on , Volume: 43 , Issue: 8 , Aug. 1994

Pages:892 - 898

[\[Abstract\]](#) [\[PDF Full-Text \(528 KB\)\]](#) **IEEE JNL**

IEEE HOME | SEARCH IEEE | SHOP | WEB ACCOUNT | CONTACT IEEE


[Membership](#) | [Publications/Services](#) | [Standards](#) | [Conferences](#) | [Careers/Jobs](#)
IEEE Xplore
RELEASE 1.3

 Welcome
 United States Patent and Trademark Office


» See

[Help](#) | [FAQ](#) | [Terms](#) | [IEEE Peer Review](#)

Quick Links

Welcome to IEEE Xplore

- ☐ Home
- ☐ What Can I Access?
- ☐ Log-out

Tables of Contents

- ☐ Journals & Magazines
- ☐ Conference Proceedings
- ☐ Standards

Search

- ☐ By Author
- ☐ Basic
- ☐ Advanced

Member Services

- ☐ Join IEEE
- ☐ Establish IEEE Web Account
- ☐ Access the IEEE Member Digital Library

IEEE Enterprise

- ☐ Access the IEEE Enterprise File Cabinet

Print Format

Your search matched **3** of **1075719** documents.A maximum of **500** results are displayed, **50** to a page, sorted by **Relevance Descending** order.**Refine This Search:**

You may refine your search by editing the current search expression or enter a new one in the text box.

rsa <and> ('chinese remainder' <or> crt)

Search

☐ Check to search within this result set**Results Key:****JNL** = Journal or Magazine **CNF** = Conference **STD** = Standard
1 The Chinese Remainder Theorem and its application in a high-speed crypto chip
Grossschadl, J.;

Computer Security Applications, 2000. ACSAC '00. 16th Annual Conference , Dec. 2000

Pages:384 - 393

[\[Abstract\]](#) [\[PDF Full-Text \(660 KB\)\]](#) IEEE CNF

2 Fast implementations of RSA cryptography
Shand, M.; Vuillemin, J.;

Computer Arithmetic, 1993. Proceedings., 11th Symposium on , 29 June-2 Ju 1993

Pages:252 - 259

[\[Abstract\]](#) [\[PDF Full-Text \(516 KB\)\]](#) IEEE CNF

3 Modified Chinese remainder theorem and its application to proxy signatures
Chuan-Kun Wu; Varadharajan, V.;

Parallel Processing, 1999. Proceedings. 1999 International Workshops on , 21 Sept. 1999

Pages:146 - 151

[\[Abstract\]](#) [\[PDF Full-Text \(188 KB\)\]](#) IEEE CNF

[Home](#) | [Log-out](#) | [Journals](#) | [Conference Proceedings](#) | [Standards](#) | [Search by Author](#) | [Basic Search](#) | [Advanced Search](#) | [Join IEEE](#) | [Web Account](#) | [New this week](#) | [OPAC Linking Information](#) | [Your Feedback](#) | [Technical Support](#) | [Email Alerting](#) | [No Robots Please](#) | [Release Notes](#) | [IEEE Online Publications](#) | [Help](#) | [FAQ](#) | [Terms](#) | [Back to Top](#)


Copyright © 2004 IEEE — All rights reserved



US Patent & Trademark Office

[Subscribe \(Full Service\)](#) [Register \(Limited Service, Free\)](#) [Login](#)Search: ☒ The ACM Digital Library ☐ The Guide

THE ACM DIGITAL LIBRARY

 [Feedback](#) [Report a problem](#) [Satisfaction survey](#)

Published since January 1947 and Published before July 2000

Found 32 of 104,690

Terms used **rsa chinese remainder crt**Sort results
byDisplay
results [Save results to a Binder](#) [Search Tips](#)☐ [Open results in a new window](#)[Try an Advanced Search](#)[Try this search in The ACM Guide](#)

Results 1 - 20 of 32

Result page: **1** [2](#) [next](#)Relevance scale ☐ ☐ ☐ ☐ ☐**1** [Finding smooth integers in short intervals using CRT decoding](#)

Dan Boneh

May 1999 **Proceedings of the thirty-second annual ACM symposium on Theory of computing**Full text available:  pdf(712.12 KB) Additional Information: [full citation](#), [references](#), [citations](#), [index terms](#)**2** [Hardware speedups in long integer multiplication](#)

M. Shand, P. Bertin, J. Vuillemin

May 1990 **Proceedings of the second annual ACM symposium on Parallel algorithms and architectures**Full text available:  pdf(939.04 KB) Additional Information: [full citation](#), [references](#), [citations](#), [index terms](#)**3** [Digital signatures for flows and multicasts](#)


Chung Kei Wong, Simon S. Lam

August 1999 **IEEE/ACM Transactions on Networking (TON)**, Volume 7 Issue 4Full text available:  pdf(268.97 KB) Additional Information: [full citation](#), [references](#), [citations](#), [index terms](#)**4** [List decoding: algorithms and applications](#)

Madhu Sudan

March 2000 **ACM SIGACT News**, Volume 31 Issue 1Full text available:  pdf(844.28 KB) Additional Information: [full citation](#), [citations](#), [index terms](#)**5** [Signature schemes based on the strong RSA assumption](#)

Ronald Cramer, Victor Shoup


November 1999 **Proceedings of the 6th ACM conference on Computer and communications security**Full text available:  pdf(530.95 KB) Additional Information: [full citation](#), [abstract](#), [references](#), [citations](#), [index terms](#)

We describe and analyze a new digital signature scheme. The new scheme is quite efficient, does not require the the signer to maintain any state, and can be proven secure against adaptive chosen message attack under a reasonable intractability assumption, the so-called strong RSA assumption. Moreover, a hash function can be incorporated into the scheme in such a way that it is also secure in the random oracle model under the standard RSA assumption.

6 On the fly signatures based on factoring

Guillaume Poupard, Jacques Stern

November 1999 **Proceedings of the 6th ACM conference on Computer and communications security**


Full text available:  pdf(786.71 KB) Additional Information: [full citation](#), [abstract](#), [references](#), [index terms](#)

In response to the current need for fast, secure and cheap public-key cryptography largely induced by the fast development of electronic commerce, we propose a new on the fly signature scheme, i.e. a scheme that requires very small on-line work for the signer. It combines provable security based on the factorization problem, short public and secret keys, short transmission and minimal on-line computation. It is the first RSA-like signature scheme that can be used for both ef ...

7 Cryptographic limitations on learning Boolean formulae and finite automata

Michael Kearns, Leslie Valiant

January 1994 **Journal of the ACM (JACM)**, Volume 41 Issue 1


Full text available:  pdf(2.26 MB) Additional Information: [full citation](#), [abstract](#), [references](#), [citations](#), [index terms](#)

In this paper, we prove the intractability of learning several classes of Boolean functions in the distribution-free model (also called the Probably Approximately Correct or PAC model) of learning from examples. These results are representation independent, in that they hold regardless of the syntactic form in which the learner chooses to represent its hypotheses. Our methods reduce the problems of cracking a number of well-known public-key cryptosystems to the l ...

8 A new public key cryptosystem based on higher residues

David Naccache, Jacques Stern


November 1998 **Proceedings of the 5th ACM conference on Computer and communications security**

Full text available:  pdf(1.00 MB) Additional Information: [full citation](#), [references](#), [citations](#), [index terms](#)

9 How to securely replicate services

Michael K. Reiter, Kenneth P. Birman

May 1994 **ACM Transactions on Programming Languages and Systems (TOPLAS)**, Volume 16 Issue 3

Full text available:  pdf(1.78 MB) Additional Information: [full citation](#), [abstract](#), [references](#), [citations](#), [index terms](#)

We present a method for constructing replicated services that retain their availability and integrity despite several servers and clients being corrupted by an intruder, in addition to others failing benignly. We also address the issue of maintaining a causal order among client requests. We illustrate a security breach resulting from an intruder's ability to effect a violation of causality in the sequence of requests processed by the service and propose an approach to counter this attack. A ...

Keywords: causality, replication, state machines, threshold cryptography

10 Efficient verifiable encryption (and fair exchange) of digital signatures

Giuseppe Ateniese


November 1999 **Proceedings of the 6th ACM conference on Computer and communications security**Full text available:  pdf(781.40 KB) Additional Information: [full citation](#), [abstract](#), [references](#), [citations](#), [index terms](#)

A fair exchange protocol allows two users to exchange items so that either each user gets the other's item or neither user does. In [2], verifiable encryption is introduced as a primitive that can be used to build extremely efficient fair exchange protocols where the items exchanged represent digital signatures. Such protocols may be used to digitally sign contracts. This paper presents new simple schemes for verifiable encryption of digital signatures. We make us ...

Keywords: contract signing problem, digital signatures, fair exchange, proof of knowledge, public-key cryptography, verifiable encryption

11 Strong signature schemes


Shafi Goldwasser, Silvio Micali, Andy Yao

December 1983 **Proceedings of the fifteenth annual ACM symposium on Theory of computing**Full text available:  pdf(691.09 KB) Additional Information: [full citation](#), [abstract](#), [references](#), [citations](#), [index terms](#)

The notion of digital signature based on trapdoor functions has been introduced by Diffie and Hellman[3]. Rivest, Shamir and Adleman[8] gave the first number theoretic implementation of a signature scheme based on a trapdoor function. If f is a trapdoor function and m a message, $f^{-1}(m)$ is the signature of m . The signature can be verified by computing $f(f^{-1}(m))$.

12 Probabilistic encryption & how to play mental poker keeping secret all partial information

Shafi Goldwasser, Silvio Micali

May 1982 **Proceedings of the fourteenth annual ACM symposium on Theory of computing**Full text available:  pdf(1.21 MB) Additional Information: [full citation](#), [abstract](#), [references](#), [citations](#)

This paper proposes an Encryption Scheme that possess the following property : An adversary, who knows the encryption algorithm and is given the cyphertext, cannot obtain any information about the clear-text. Any implementation of a Public Key Cryptosystem, as proposed by Diffie and Hellman in [8], should possess this property. Our Encryption Scheme follows the ideas in the number theoretic implementations of a Public Key Cryptosystem due to Rivest, Shamir and Adleman ...

13 Witness-based cryptographic program checking and robust function sharing

Yair Frankel, Peter Gemmell, Moti Yung

July 1996 **Proceedings of the twenty-eighth annual ACM symposium on Theory of computing**Full text available:  pdf(1.13 MB) Additional Information: [full citation](#), [references](#), [citations](#), [index terms](#)**14 On the generation of multivariate polynomials which are hard to factor**

Adi Shamir


June 1993 **Proceedings of the twenty-fifth annual ACM symposium on Theory of computing**

Full text available:  pdf(770.06 KB) Additional Information: [full citation](#), [references](#), [citations](#), [index terms](#)

15 On-line textile designing

Janice R. Lourie, John J. Lorenzo, Abel Bomberault

January 1966 **Proceedings of the 1966 21st national conference**


Full text available:  pdf(791.03 KB) Additional Information: [full citation](#), [abstract](#), [references](#), [citations](#), [index terms](#)

Woven fabric is formed from two sets of threads such that all the threads in one set are parallel to each other and perpendicular to all threads in the other set. The set of threads which run the length of the fabric is called the warp; the set of crosswise threads is called the weft. These two sets of threads are interwoven to form a mesh which is called a web. The design of a woven fabric originates with an artist's sketch. Since the threads within each set remain parallel to e ...

16 Functional partitioning improvements over structural partitioning for packaging constraints and synthesis: tool performance

Frank Vahid, Thuy Dm Le, Yu-Chin Hsu

April 1998 **ACM Transactions on Design Automation of Electronic Systems (TODAES)**, Volume 3 Issue 2

Full text available:  pdf(225.74 KB) Additional Information: [full citation](#), [abstract](#), [references](#), [citations](#), [index terms](#)


Incorporating functional partitioning into a synthesis methodology leads to several important advantages. In functional partitioning, we first partition a functional specification into smaller subspecifications and then synthesize structure for each, in contrast to the current approach of first synthesizing structure for the entire specification and then partitioning that structure. One advantage is the improvement in I/O performance and package count, when partitioning among hardware block ...

Keywords: behavioral synthesis, functional partitioning, system-level design

17 Anonymous authentication with subset queries (extended abstract)

Dan Boneh, Matt Franklin

November 1999 **Proceedings of the 6th ACM conference on Computer and communications security**

Full text available:  pdf(613.93 KB) Additional Information: [full citation](#), [abstract](#), [references](#), [citations](#), [index terms](#)

We develop new schemes for anonymous authentication that support identity escrow. Our protocols also allow a prover to demonstrate membership in an arbitrary subset of users; key revocation is an important special case of this feature. Using the Fiat-Shamir heuristic, our interactive authentication protocols yield new constructions for non-interactive group signature schemes. We use the higher-residuosity assumption, which leads to greater efficiency and more natural security proofs than pr ...

Keywords: anonymous authentication, group signature, identity escrow

18 Secure group communications using key graphs

Chung Kei Wong, Mohamed Gouda, Simon S. Lam

February 2000 **IEEE/ACM Transactions on Networking (TON)**, Volume 8 Issue 1

Full text available:  pdf(345.54 KB) Additional Information: [full citation](#), [references](#), [citations](#), [index terms](#), [review](#)

Keywords: confidentiality, group communications, group key management, key distribution, multicast, privacy, rekeying, security

19 Multicast security and its extension to a mobile environment

Li Gong, Nachum Shacham

March 1995 **Wireless Networks**, Volume 1 Issue 3

Full text available:  pdf(1.22 MB) Additional Information: [full citation](#), [abstract](#), [references](#), [citations](#)

Multicast is rapidly becoming an important mode of communication and a good platform for building group-oriented services. To be used for trusted communication, however, current multicast schemes must be supplemented by mechanisms for protecting traffic, controlling participation, and restricting access of unauthorized users to data exchanged by the participants. In this paper, we consider fundamental security issues in building a trusted multicast facility. We discuss techniques for group- ...



20 25 years of quantum cryptography

Gilles Brassard, Claude Crépeau

September 1996 **ACM SIGACT News**, Volume 27 Issue 3

Full text available:  pdf(918.87 KB) Additional Information: [full citation](#), [abstract](#), [citations](#), [index terms](#)

The fates of *SIGACT News* and Quantum Cryptography are inseparably entangled. The exact date of Stephen Wiesner's invention of "conjugate coding" is unknown but it cannot be far from April 1969, when the premier issue of *SIGACT News*---or rather *SIGACT News* as it was known at the time---came out. Much later, it was in *SIGACT News* that Wiesner's paper finally appeared [74] in the wake of the first author's early collaboration with Charles H. Bennett [7]. It was also in < ...



Results 1 - 20 of 32

Result page: [1](#) [2](#) [next](#)

The ACM Portal is published by the Association for Computing Machinery. Copyright © 2004 ACM, Inc.

[Terms of Usage](#) [Privacy Policy](#) [Code of Ethics](#) [Contact Us](#)

Useful downloads:  [Adobe Acrobat](#)  [QuickTime](#)  [Windows Media Player](#)  [Real Player](#)



Web Images Groups News Froogle [more »](#)

"chinese remainder theorem" ("hensel lifting"

Search

[Advanced Search](#)
[Preferences](#)

Web Results 1 - 10 of about **29** for "**chinese remainder theorem**" ("**hensel lifting**" OR "**hensle lifting**") **rsa e**

Did you mean: "chinese remainder theorem" ("hensel lifting" OR "**hensel** lifting") **rsa exponent**

[PPT] Efficient Cryptography

File Format: Microsoft Powerpoint 97 - [View as HTML](#)

... 2. **RSA** Decryption using **Chinese Remainder Theorem**. n. ... p_2 . $Mp_2 = M \bmod p_2$. The decryption of Multi-**Exponent RSA** can be computed. ... **Hensel lifting**. **Hensel Lifting**. ...

www.informatik.tu-darmstadt.de/TI/Lehre/SS04/Vorlesung/EK/lecture9.ppt - [Similar pages](#)

[PDF] Efficient Cryptography

File Format: PDF/Adobe Acrobat - [View as HTML](#)

... is equal to M from the **Chinese remainder theorem**, because both ... this exercise shows that the **Hensel lifting** can be ... 4. Exercise (Multi-**Exponent RSA** with $n = p_2 q$...

www.informatik.tu-darmstadt.de/TI/Lehre/SS04/Vorlesung/EK/answer9.pdf - [Similar pages](#)

[[More results from www.informatik.tu-darmstadt.de](#)]

[PDF] Lattice Attacks in Cryptography

File Format: PDF/Adobe Acrobat - [View as HTML](#)

... Definitions Reduced Bases Algorithmic Problems 2 Example GnuPG 3 Proposal Index
Calculus Method Symmetric Representation Fast **RSA** Variants Provable Bounds for ...

www.cs.uwaterloo.ca/~mjhinek/comps-palegoldenrod.pdf - [Similar pages](#)

[PDF] LNCS 3089 - Security Analysis of CRT-Based Cryptosystems

File Format: PDF/Adobe Acrobat

... on the implementation using the **Chinese remainder theorem** (CRT), which ... from modulo p using fast **Hensel lifting**, and the ... time of Multi- **Exponent RSA** is faster ...

www.springerlink.com/index/5LA2JHK34Y77CL73.pdf - [Similar pages](#)

[PDF] An Advantage of Low-Exponent RSA with Modulus Primes Sharing Least ...

File Format: PDF/Adobe Acrobat

... prime factors of N, the **Chinese Remainder Theorem** (CRT) can ... An Advantage of Low-**Exponent**

RSA with Modulus Primes Sharing LSBs 57 **Hensel lifting** to show ...

www.springerlink.com/index/Y4V8FC0HLK8PPWHF.pdf - [Similar pages](#)

[PDF] A Practical Public Key Cryptosystem from Paillier and Rabin ...

File Format: PDF/Adobe Acrobat - [View as HTML](#)

... Then, by using the **Chinese Remainder Theorem**, we obtain an s ... Proof: From the **Hensel-lifting**, the set of quadratic residues ... 6]. In [6], given an **RSA** modulus n ...

www-ma4.upc.es/~dgalindo/PKC2003-final.pdf - [Similar pages](#)

[PDF] An efficient semantically secure elliptic curve cryptosystem based ...

File Format: PDF/Adobe Acrobat - [View as HTML](#)

... $E_{p_2}(a, b)$ and $E_{q_2}(a, b)$. Via the **Chinese Remainder Theorem** E_{n_2} ... **RSA**[n, n] is hard, where **RSA**[n, e] denotes the **RSA** function with **exponent** e. To ...

www-ma4.upc.es/~dgalindo/kmovdam.pdf - [Similar pages](#)

[PDF] Cryptobytes - Volume 5, No. 1, Winter/Spring 2002

File Format: PDF/Adobe Acrobat - [View as HTML](#)

... $p-1)(q-1)$. The value e is called the encryption **exponent**, and is ... It is standard practice

to employ the **Chinese Remainder Theorem** (CRT) for **RSA** decryption. ...

www.rsasecurity.com/rsalabs/cryptobytes/CryptoBytes_January_2002_final.pdf - [Similar pages](#)

 **[PDF]** [Tunable balancing of RSA – Preliminary discussion draft](#)

File Format: PDF/Adobe Acrobat - [View as HTML](#)

... are performed using the **Chinese remainder theorem** (CRT), cost ... 1024-bit moduli) for **RSA** decryption, but ... public exponents (otherwise the **Hensel lifting** is slow ...

www.cs.upb.de/cs/ag-bloemer/personen/alex/vortraege/material/short-rsa.pdf - [Similar pages](#)

[PS] [SOLVING SIMULTANEOUS MODULAR EQUATIONS OF LOW DEGREE](#)

File Format: Adobe PostScript - [View as Text](#)

... to a single equation using the **chinese remainder theorem**. ... Now apply **Hensel lifting** to obtain these factors modulo ... linearly related messages using **RSA** with low ...

www.nada.kth.se/~johanh/rsalowexponent.ps - [Similar pages](#)

Did you mean to search for: ["chinese remainder theorem"](#) (["hensel lifting"](#) OR ["***hensel* lifting**"](#)) [rsa exponent](#)

Google 

Result Page: 1 2 3 [Next](#)

[Search within results](#) | [Language Tools](#) | [Search Tips](#) | [Dissatisfied? Help us improve](#)

[Google Home](#) - [Advertising Programs](#) - [Business Solutions](#) - [About Google](#)

©2004 Google